Kaspersky Endpoint Detection and Response Optimum

Lleve sus defensas de endpoints al siguiente nivel y afronte las amenazas evasivas de frente, sin complicaciones.

kaspersky 25 years

Kaspersky Endpoint Detection and Response Optimum

Es hora de subir de nivel. Tiene todo listo, no solo para proteger su organización con las tecnologías antimalware esenciales, sino también para identificar, analizar y neutralizar de manera eficaz esas amenazas que están específicamente diseñadas para evadir la protección tradicional y quedar ocultas en lo profundo de los sistemas, preparadas para hacer el mayor daño posible.

Los desafíos

Amenazas que evaden detecciones

El malware, ransomware, spyware y otras amenazas evasivas son cada vez más inteligentes en evitar los mecanismos de detección tradicional, ya que usan herramientas de sistemas legítimos y otras técnicas avanzadas para atacar.

El 64 % de las organizaciones ya fueron víctimas de ataques de ransomware. El 79 % de ellas pagaron el rescate a sus atacantes.

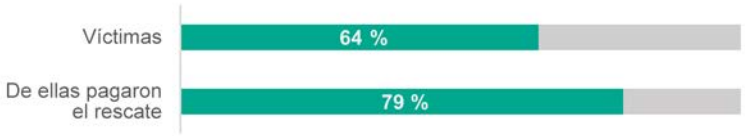
Kaspersky, mayo de 2022

Ransomware como servicio

Los hackers pueden adquirir herramientas ya desarrolladas muy económicas y atacar a cualquier persona para robar datos, dañar infraestructuras y exigir grandes cantidades de dinero.

Recursos limitados

Las infraestructuras son cada vez más complejas y abarcadoras, mientras que los recursos (tiempo, dinero y atención) escasean. Aquí no hay espacio para recursos que no se usan.



"Apreciamos las soluciones integrales de Kaspersky, su confiabilidad y su servicio y asistencia rápidos. Garantizan la disponibilidad de nuestro entorno de TI".

Marcelo Mendes CISO, NEO
Leer estudio de caso

Cómo podemos ayudar

Kaspersky Endpoint Detection and Response (EDR) Optimum le ayuda a identificar, analizar y neutralizar las amenazas evasivas gracias a que proporciona detección avanzada fácil de usar, investigación simplificada y respuesta automatizada.

Protección avanzada

Nuestros mecanismos de detección avanzados incluyen tecnologías de aprendizaje automático, análisis del comportamiento y entornos de pruebas de nube, entre otros.

Las sencillas herramientas de análisis visual permiten que comprenda en su totalidad la amenaza y su alcance y responda rápidamente para evitar el ataque antes de que se produzcan daños.

Una solución

La seguridad de endpoints avanzada se integra a un producto EDR fácil de usar para una mayor protección de computadoras portátiles, estaciones de trabajo, servidores, cargas de trabajo en la nube y entornos virtuales.

La implementación y la administración ocurre en un solo lugar, a través de una única consola local o en la nube.

Sencillo y eficaz

Desarrollamos EDR Optimum pensando en pequeños equipos de ciberseguridad que buscan mejorar sus capacidades de respuesta ante incidentes y desarrollar habilidades, pero no cuentan con mucho tiempo.

Automatizamos y optimizamos la mayoría de las tareas a fin de que tenga más tiempo para dedicar a lo que en verdad importa.

Principales ventajas

- **Evite diversos tipos** de amenazas
- **Proteja sus sistemas y datos** de amenazas evasivas
- **Descubra amenazas actuales** antes de que actúen
- **Reconozca amenazas evasivas** en todos los endpoints
- **Comprenda la amenaza** y analícela con rapidez
- **Evite daños** con una respuesta rápida y automatizada
- **Ahorre tiempo y recursos** con una herramienta simplificada
- **Defienda todos los endpoints:** ordenadores portátiles, servidores, cargas de trabajo en la nube

Características principales

- Seguridad de endpoints **avanzada e inherente**
- **Detección avanzada** basada en el aprendizaje automático
- **Análisis de indicadores de compromiso** (IOC)
- **Herramientas de investigación** y análisis visuales
- Todos los datos necesarios en **una única tarjeta de alerta**
- **Guía de respuestas y** automatización incorporadas
- **Consola local o en una única nube** y automatización
- Compatibilidad con **estaciones de trabajo, servidores virtuales y físicos, implementaciones VDI y cargas de trabajo en nubes públicas**

Casos de uso clave

¿Me estarán atacando?

- **Detección avanzada**: se basa en el aprendizaje automático, incluye entornos de pruebas de nube y detecta amenazas de forma automática.
- **Descargue y analice IoC** desde securelist.com u otras fuentes para encontrar amenazas avanzadas.

¿Puedo neutralizarlas?

- **Emplee diversas opciones de respuesta**: aísle el host, impida la ejecución de archivos o elimínelos.
- **Analice otros host** en busca de indicios de una amenaza analizada.
- **Aplique respuestas automáticas** en diversos host para descubrir la amenaza (IoC).

¿Cómo puedo capacitarme?

- **Consulte nuestra guía de respuestas** en la tarjeta de alerta.
- **Acceda a Threat Intelligence Portal** y las novedades respecto de la tecnología de la información.
- **Mejore su experiencia** a medida que analiza y responde a las amenazas.

¿Cómo ha sucedido?

- Analice la amenaza en un **árbol de procesamiento visual.**
- Haga un seguimiento de sus acciones en **un gráfico con desgloses.**
- **Comprenda la causa principal y conozca el punto de entrada** a la infraestructura.

¿Cómo evito que vuelva a ocurrir?

- **Aplique la información que aprendió:** sepa qué direcciones IP y sitios web debe bloquear, qué políticas debe modificar y a qué empleados debe capacitar.
- **Redacte reglas para evitar dichas amenazas en el futuro;** por ejemplo, evite la ejecución de archivos.

¿Qué ocurre con las amenazas a los bienes?

- **La seguridad de endpoints avanzada** está preparada para detener la mayoría de las amenazas de inmediato.
- **Mejore su capacidad de aplicar parches** con la administración de vulnerabilidades y parches.
- **Automatice la reducción de la superficie de ataque** y ajuste políticas al controlar endpoints.

Funcionamiento

Para obtener una demostración rápida, vea este video.

¿De dónde viene?

Ya tiene una defensa contra el malware, ¿pero no es suficiente?

Mejore su protección de endpoints

Ya sea que use una protección de endpoints de Kaspersky o de un tercero, este es el momento adecuado para pensar en implementar un producto de detección y respuesta de endpoints.

No se trata solo de funcionalidades avanzadas, sino de tener todo preparado frente a amenazas evasivas, que implica identificarlas, analizarlas y neutralizarlas.

Obtenga más información sobre cómo protegerse de amenazas evasivas en Una guía del usuario para un nivel óptimo de seguridad.

¿Ya usa productos de Kaspersky?

Optimice su seguridad

Mejoramos nuestros productos todo el tiempo, por lo que debe asegurarse de tener las últimas actualizaciones o migrar a la nube y olvidarse por completo de tareas rutinarias y molestas.

En la última versión de Kaspersky EDR Optimum, encontrará:

- Una respuesta guiada en una tarjeta de alerta
- La respuesta a una verificación de objetos de sistemas críticos antes de solicitarla
- Un archivo de reputación sobre inteligencia de amenazas en una tarjeta de alerta
- Análisis de profundidad ilimitada del árbol de procesos

Obtenga más información sobre las nuevas características aquí.

¿Eres nuevo en Kaspersky?

Optimice su seguridad

Miles de empresas en todo el mundo utilizan Kaspersky EDR Optimum por las siguientes razones:

- Un único producto comprende una plataforma de protección de endpoints potente y funciones básicas de detección y respuesta de endpoints.
- Cuenta con funciones de detección y respuesta de endpoints fáciles de usar, diseñadas para pequeños equipos de ciberseguridad.
- Se trata de una solución liviana y flexible con la posibilidad de implementarla de forma local o en la nube.

Descubra Kaspersky Optimum Security, una solución compuesta para amenazas evasivas, basada en tecnología de EDR y MDR.

Avance con un enfoque por etapas

Las herramientas que usa deberían ser las adecuadas para sus necesidad empresariales y de ciberseguridad, y para sus equipos y recursos. Es por ello que simplificamos el proceso de elección del nivel de ciberseguridad que es su principal preocupación ahora: contamos con tres opciones diferentes según el perfil de su organización.

Kaspersky Security Foundations

Bloquee automáticamente gran parte de las amenazas

- Prevención automatizada multivectorial de los incidentes que provocan las amenazas básicas, que suponen la gran mayoría de los ciberataques.
- Esta es la etapa básica para empresas de cualquier tamaño y complejidad en el desarrollo de una estrategia de defensa integrada.
- Protección fiable de los terminales para quienes tienen equipos de TI pequeños y conocimientos de seguridad incipientes.

» Más información

Kaspersky Optimum Security

Mejora de las defensas frente las amenazas evasivas si tiene:

- Una empresa con un pequeño equipo de seguridad de TI con conocimientos técnicos básicos de ciberseguridad.
- Un entorno de TI que crece en tamaño y complejidad, lo que aumenta la superficie de ataque.
- Falta de recursos de ciberseguridad y necesidad de una mayor protección.
- Una necesidad creciente de desarrollar una capacidad de respuesta ante incidentes.

» Más información

Kaspersky Expert Security

Preparación frente a ataques complejos y similares a APT para organizaciones.

- Con entornos de TI complejos y distribuidos.
- Con un equipo de seguridad de TI maduro, o un centro de operaciones de seguridad (SOC) establecido.
- Con poca tolerancia al riesgo por los altos costes de los incidentes de seguridad y las filtraciones de datos.
- Con actividades en un sector donde el cumplimiento de las regulaciones es una preocupación

» Más información

Quiénes somos

Somos una empresa de ciberseguridad privada internacional con miles de clientes y socios en todo el mundo y nos comprometemos a ser **transparentes e independientes**. Desarrollamos herramientas y brindamos servicios desde hace 25 años para mantener su seguridad con nuestras **tecnologías más probadas y más premiadas**.

IDC

Evaluación de proveedores de IDC MarketScape sobre seguridad de endpoints moderna y global para empresas y pymes en 2021

Competidor principal

AV-Test

Protección avanzada de endpoints: Prueba de protección de ransomware

Protección 100%

Radicati Group

Cuadrante de mercado sobre amenazas persistentes avanzadas (APT)

Mejor competidor

Si necesita más

Revise **Kaspersky EDR Expert**, una potente herramienta de EDR para brindarles a sus especialistas capacidades de búsqueda exhaustiva de amenazas, mecanismos de amplia personalización y de detección superior.

Eche un vistazo más de cerca

Para obtener más información sobre cómo Kaspersky EDR Optimum aborda las ciberamenazas al mismo tiempo que facilita el uso de su equipo de seguridad y sus recursos, visite **www.kaspersky.es/enterprise-security/edr-security-software-solution**

Noticias sobre amenazas cibernéticas: securelist.com
Noticias de seguridad de TI: business.kaspersky.com
Seguridad de TI para PYMES: kaspersky.com/business
Seguridad de TI para grandes empresas: kaspersky.com/enterprise

kaspersky.es